From: D. J. Bernstein <djb@cr.yp.to>
Sent: Saturday, June 8, 2019 4:46 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: [pqc-forum] ROUND 2 OFFICIAL COMMENT: SABER
Attachments: signature.asc

There are at least two problems with the first Saber theorem, Theorem 6.1. (Also with Round5 Theorem 2.6.1, which copied the Saber theorem and proof, modulo tweaks for the Round5 details; I won't bother filing this as a separate comment.)

1. Formally, the theorem statement is trivially correct and useless, since the statement fails to require an _efficient_ reduction. The most useful fix from the perspective of reviewers is to define the specific reductions before the theorem, and then use those definitions in the theorem statement.

2. More fundamentally, instead of claiming

   * security of Saber.PKE against all IND-CPA attacks under two
     Mod-LWR assumptions and a standard-model PRF assumption,

the theorem has to be weakened to claim merely

   * security of Saber.PKE against _ROM_ IND-CPA attacks under Mod-LWR
     assumptions.

In other words, cryptanalysts have to check not merely whether the hash function is a PRF, but whether the hash function as used inside the PKE enables any sort of non-ROM IND-CPA attacks.

Section 4.1 of my latticeproofs paper pinpoints the proof error. I'm not saying that I vouch for the correctness and applicability of the theorem with the above changes; I did only a sanity check, not a serious review.

---Dan